Xarxa de col·laboració

3. CONSELLS DE SEGURETAT

3.1 Seguretat en les aplicacions de missatgeria instantània

L'ús diari de les aplicacions de missatgeria instantània te associats uns riscos de seguretat que cal conèixer per poder-los evitar. Us adjuntem els principals riscos de seguretat i recomanacions per evitar-los.

Riscos de seguretat més comuns associats a l'ús de les aplicacions de missatgeria instantània:

- Infecció del dispositiu: quan un ciberdelinqüent accedeix remotament al vostre dispositiu i aconsegueix monitoritzar les vostres accions. Això pot perjudicar el funcionament de l'aparell o robar-ne informació.

- Fuita o robatori d'informació: perdreu la confidencialitat de la vostra informació, la qual anirà a parar a mans alienes.

- Suplantació d'identitat: amb les dades personals que obtinguin els delinqüents es faran passar per vosaltres per cometre algun tipus de delicte.

- Sessions sense tancar: si no tanqueu la vostra sessió algú altre pot accedir a les vostres dades.

- Infecció del dispositiu amb codi maliciós: es tracta d'un programari o arxiu que s'instal·la sense coneixement de l'usuari i intenta accedir a les vostres dades personals, com ara les credencials d'accés als serveis bancaris en línia.

- Ubicació dels dispositius: si teniu les opcions activades, altres persones podran saber on sou i us podran localitzar encara que vosaltres no ho vulgueu.

Recomanacions per evitar els riscos:

- Informeu-vos sobre tots els riscos de seguretat i les principals amenaces més comuns en les aplicacions de missatgeria instantània.

- Conegueu les característiques i les funcionalitats de seguretat dels vostres dispositius.

- Configureu els programes de forma adequada:

  activeu les opcions de privacitat,

  no emmagatzemeu contrasenyes

  activeu la protecció antivirus per a missatgeria.

- Mantingueu els programes i els antivirus actualitzats amb la finalitat de tancar possibles forats de seguretat.

- Desconfieu de fitxers i enllaços, especialment d'aquells que no heu sol·licitat o dels que heu rebut de desconeguts.

- Tanqueu les sessions obertes a webs, aplicacions i serveis web.

Telegram: ubicació del dispositiu

Telegram ha afegit en les seves últimes actualitzacions una nova utilitat anomenada "Persones properes". Aquesta utilitat ve per defecte desactivada, però si l'habiliteu podreu veure la ubicació dels vostres contactes i ells podran veure on us trobeu vosaltres.

Amb aquesta utilitat qualsevol altra persona propera al vostre dispositiu, amb l'ajuda d'altres aplicacions no gaire sofisticades, podria saber la posició exacta de la vostra ubicació

Com s'activa la ubicació?

Accediu al menú de Telegram.

Feu clic a "Gent propera".

En la següent pantalla feu clic a "Permet l'accés"; el dispositiu us demanarà permisos, accepteu i ja hi tindreu accés.

Quan permeteu l'accés ja podreu veure altres usuaris o usuàries de Telegram propers a vosaltres i a quina distancia es troben. En aquest punt encara no sou visibles per a la resta. Per ser-ho, feu clic a "Fes-me visible".

Com podeu tornar a ocultar la vostra ubicació a Telegram?

Accediu al menú de Telegram.

Premeu a "Gent propera".

En la següent pantalla us mostrarà l'opció "Deixar de ser visibles", en fer clic ja no sereu visibles.

WhatsApp: suplantació i segrest

Suplantació de Whatsapp

Rebeu un missatge de correu electrònic suposadament de part de Whatsapp on us demana clicar en un enllaç per fer una còpia de segurtat de tots els vostres missatges i de l'historial de trucades. Aquest enllaç us instal·la programari maliciós i us infecta el dispositiu.

Segrest de Whatsapp

Algunes aplicacions de banca electrònica, xarxes socials o les que fan servir l'IDCAT SMS, utilitzen com a mesura de seguretat avançada l'enviament de codis de seguretat i contrasenyes per missatges de text al mòbil de la persona usuària.

Aquests codis de seguretat i contrasenyes no els heu de compartir amb ningú, ja que podríeu estar donant, de forma involuntària, el control total de l'aplicació a terceres persones.

En el cas de Whatsapp, els darrers mesos s'ha detectat un increment dels intents de robatori de comptes per part de ciberdelinqüents mitjançant un atac de suplantació d'identitat, amb les dades personals que obtenen els delinqüents es fan passar per vosaltres per cometre algun tipus de delicte.

Font: Consells de Seguretat cos Mossos d'Esquadra, enllaç.